ISSN 1995-0802, Lobachevskii Journal of Mathematics, 2018, Vol. 39, No. 7, pp. 957–960. © Pleiades Publishing, Ltd., 2018.

Quantum-Assisted Blockchain

F. M. Ablayev[1*], D. A. Bulychkov[1,2], D. A. Sapaev[1,3***], A. V. Vasiliev[1****], and M. T. Ziatdinov[1*****]**

(Submitted by A. M. Elizarov)

[1] *Institute of Computational Mathematics and Information Technologies, Kazan (Volga region) Federal University, ul. Kremlevskaya 35, Kazan, Tatarstan, 420008 Russia*

[2] *Sberbank, Center of Technological Innovations, ul. Vavilova 19, Moscow, 117312 Russia*

[3] *Sberbank-Technologies, Development Department of Center of Technological Innovations, ul. Universitetskaya 7, Innopolis, 420500 Russia*

Received December 6, 2017

Abstract—Bitcoin and blockchain in general is a hot topic nowadays. In the paper we propose a quantum empowering of this technology and show how to speed-up the mining procedure using the modified Grover's algorithm.

DOI: 10.1134/S1995080218070028

Keywords and phrases: *Quantum computation, blockchain, quantum mining, Grover search.*

1. INTRODUCTION

Quantum computing is a hot modern topic of Theoretical Computer Science. Theoretical research in this area started in the last decades of the previous century. Yuri Manin and Richard Feynman were one of the first famous researchers who proposed this area of research in the 1980s. Recent results in quantum computations and quantum technology achievements brought theoretical results to the practice. The appearance of the so-called IBM-Q device created a new quantum computer science community and gave it a tool to verify the known theoretical ideas and algorithms. Another hot area in applied computer science is the blockchain technology. Clearly, that it will be interesting to check out what opportunities can quantum computation theory and quantum technology give to the blockchain technology. For instance, there were several proposals on empowering Bitcoin Electronic Cash System with quantum technologies (see, e.g. [1–3]), as well as on possible attacks on this system [4].

In this paper, we consider the natural idea of applying Grover's quantum search algorithm to the general blockchain technology (for mining). So, the paper is devoted to developing and testing this idea for the blockchain technology.

2. PRELIMINARIES

In the classical case, the complexity of searching in an unstructured data set of size n is $O(n)$, e.g., in the worst case, we have to look through all the records. The well-known Grover's algorithm [5] allows solving this problem in $O(\sqrt{n})$ steps. Thus, if we have 40 bits and we need to find a combination that satisfies a certain condition, then in the classical case we need to process about 1 000 000 000 000 different combinations, whereas the quantum algorithm will yield a result in about 1 000 000 queries. We briefly recall the structure of the algorithm.

*E-mail: fablayev@gmail.com
**E-mail: bulda@narod.ru
***E-mail: d.a.sapaev@gmail.com
****E-mail: alexander.ksu@gmail.com
*****E-mail: gltronred@gmail.com